

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

MARIA FERNANDA CASTELLANOS
RAMIREZ, et al.,

Plaintiffs, v.

LEXIS NEXIS RISK SOLUTIONS,

Defendant.

Case No. 1:22-cv-05384

PLAINTIFFS' RESPONSE IN OPPOSITION TO
DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

INTRODUCTION	1
FACTUAL BACKGROUND	2
I. ARGUMENT	4
A. The complaint sufficiently alleges LexisNexis’ conduct violates the ICFA.	5
1. Plaintiffs have an obvious “consumer nexus” to LexisNexis’ unfair business practice of gathering, aggregating, and selling their private data to third parties.	5
2. Plaintiffs have adequately alleged LexisNexis’ conduct qualifies as an unfair business practice under the ICFA	8
3. Plaintiffs adequately pled actual damages	12
B. Plaintiffs Sufficiently Plead Their Claim for Unjust Enrichment.....	14
C. Plaintiffs Sufficiently Plead Their Claim for Intrusion Upon Seclusion	15
D. Plaintiffs Sufficiently Alleged Facts Establishing Associational Standing	19
CONCLUSION	20

TABLE OF AUTHORITIES

CASES

<i>Athey Prods. Corp. v. Harris Bank Roselle</i> , 89 F.3d 430 (7th Cir. 1996)	6, 7
<i>Bank One Milwaukee v. Sanchez</i> , 783 N.E.2d 217 (Ill. App. Ct. 2003)	6
<i>Berry v. LexisNexis Risk & Info. Analytics Grp., Inc.</i> , No. 3:11-CV-754, 2014 WL 4403524 (E.D. Va. Sept. 5, 2014)	12
<i>Brooks v. Thomson Reuters Corp.</i> , No. 21-cv-01418-EMC, 2021 WL 3621837 (N.D. Cal. Aug. 16, 2021)	1, 9, 19
<i>Calhoun v. Google LLC</i> , 526 F. Supp. 3d 605 (N.D. Cal. 2021)	13, 17
<i>Callahan v. PeopleConnect, Inc.</i> , No. 20-CV-09203-EMC, 2021 WL 5050079 (N.D. Cal. Nov. 1, 2021)	13, 14
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018)	4, 17
<i>Centerline Equipment Corp. v. Banner Personnel Service, Inc.</i> , 545 F. Supp. 2d 768 (N.D. Ill. 2008)	9, 12, 13
<i>Deerpath Consol. Neighborhood Ass'n v. Lake County Bd. of Review</i> , No. 2-19-0985, 2021 WL 5998539, at *4 (Ill. App. Ct. Dec. 20, 2021)	20
<i>Duncan Place Owners Ass'n v. Danze, Inc.</i> , 927 F.3d 970 (7th Cir. 2019)	20
<i>Frazier v. U.S. Bank Nat. Ass'n</i> , No. 11 C 8775, 2013 WL 1385612 (N.D. Ill. Apr. 4, 2013)	6, 7
<i>FTC v. Sperry & Hutchinson Co.</i> , 405 U.S. 233 (1972)	10
<i>Gaston v. LexisNexis Risk Solutions, Inc.</i> , 483 F. Supp. 3d 318 (W.D.N.C. 2020)	12
<i>Gaston v. LexisNexis Risk Solutions, Inc.</i> , No. 5:16-cv-00009-KBD-DCK, 2021 WL 2077812 (W.D.N.C., May 24, 2021)	12
<i>Global Total Office Ltd. Partnership v. Global Allies, LLC</i> ,	

No. 10 C 1896, 2011 WL 3205487 (N.D. Ill. July 28, 2011)	7
<i>Gross v. Chapman</i> , 475 F. Supp. 858 (N.D. Ill. 2020)	18
<i>Hope Clinic for Women, Ltd. v. Flores</i> , 991 N.E.2d 745 (Ill. 2013)	4
<i>HPI Health Care Services, Inc. v. Mt. Vernon Hospital, Inc.</i> , 545 N.E.2d 672 (Ill. 1989)	14
<i>In re Facebook, Inc., Consumer Priv. User Profile Litig.</i> , 402 F. Supp. 3d 767 (N.D. Cal. 2019)	18
<i>In re Michaels Store Pin Pad Litig.</i> , 830 F.Supp.2d 518 (N.D. Ill. 2011)	6
<i>In re Nickelodeon Consumer Privacy Litigation</i> , 827 F.3d 262 (3d Cir. 2016)	17
<i>In re Trans Union Corp. Privacy Litig.</i> , 326 F. Supp. 2d 893 (N.D. Ill. 2004)	16, 17
<i>Johnson v. K mart Corp.</i> , 723 N.E.2d 1192 (Ill. App. Ct. 2000)	15
<i>Kellman v. Spokeo, Inc.</i> , No. 3:21-CV-08976-WHO, 2022 WL 1157500 (N.D. Cal. Apr. 19, 2022)	13, 14
<i>Lawlor v. North Am. Corp. of Illinois</i> , 983 N.E.2d 414 (Ill. 2012)	15
<i>Leopold v. Levin</i> , 259 N.E.2d 250 (Ill. 1970)	5
<i>McConchie v. Scholz</i> , 567 F.Supp.3d 861 (N.D. Ill. 2021)	20
<i>McDonald v. Kiloo ApS</i> , 385 F.Supp.3d 1022 (N.D. Cal. 2019)	17
<i>Midcoast Aviation, Inc. v. General Elec. Credit Corp.</i> , 907 F.2d 732 (7th Cir. 1990)	14
<i>Newman v. Metropolitan Life Insurance Co.</i> , 885 F.3d 992 (7th Cir. 2018)	12

<i>Opperman v. Path, Inc.</i> , 205 F.Supp.3d 1064 (N.D. Cal. 2016)	17
<i>People ex rel. Fahner v. Hedrich</i> , 438 N.E.2d 924 (Ill. App. Ct. 1982)	10
<i>People ex rel. Mosk v. Nat’l Rsch. Co. of Cal.</i> , 20 Cal. Rptr. 516 (Cal. Dist. Ct. App. 1962)	9
<i>People v. Nat’l Ass’n of Realtors</i> , 174 Cal. Rptr. 728 (Cal. Ct. App. 1981)	9
<i>Prairie Rivers Network v. Dynegy Midwest Generation, LLC</i> , 2 F.4th 1002 (7th Cir. 2021)	20
<i>Retired Chi. Police Ass’n v. City of Chicago</i> , 7 F.3d 584, 603 (7 th Cir. 1993)	20
<i>Robinson v. Toyota Motor Credit Corp.</i> , 775 N.E.2d 951 (Ill. 2002)	8
<i>Spiegel, Inc. v. FTC</i> , 540 F. 2d 287 (7th Cir. 1976)	10
<i>Thornley v. Clearview AI, Inc.</i> , 984 F.3d 1241 (7th Cir. 2021)	13
<i>Totty v. Anderson Funeral Home, Ltd.</i> , 448 F. Supp. 3d 928 (N.D. Ill. 2020) (Rowland, J.)	8
<i>U.S. Dep’t of Def. v. Fed. Lab. Rels. Auth.</i> , 510 U.S. 487 (1994)	4
<i>U.S. Dep’t of Just. v. Reps. Comm. For Freedom of Press</i> , 489 U.S. 749 (1989)	1, 4, 19
<i>U.S. Dep’t of State v. Ray</i> , 502 U.S. 164 (1991)	4
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	20
<u>STATUTES</u>	
California’s Unfair Competition Law (UCL)	9

Chicago’s Welcoming City Ordinance	5,10
Cook County, Ill., Code of Ordinances ch. 46, art. II, div. 1, subdiv. I, § 46-37	5
Cook County’s Detainer Ordinance.....	5,10
Driver’s Privacy Protection Act (DPPA) (18 U.S.C. § 2721 2000))	12
Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681 et. seq.).....	12
5 Ill. Comp. Stat. § 805/15	5
815 Ill. Comp. Stat. § 505/10.....	6
815 Ill. Comp. Stat. § 505/11	6
815 Ill. Comp. Stat. § 530/2	9
815 Ill. Comp. Stat. § 530/5	11
Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA)	passim
Illinois Personal Information Protection Act (PIPA).....	11
Illinois TRUST Act.....	5,10
Municipal Code of Chicago § 2-173-020	5
Municipal Code of Chicago § 2-173-030	5
Municipal Code of Chicago § 2-173-042	5
United States Code Title 15 Section 45	9
United States Code Title 18 Section 2702	12
United States Code Title 18 Section 2703	12
United States Code Title 47 Section 551	12

RULES

Fed. R. Civ. P. 15(a)(2).....	20
-------------------------------	----

TREATISES

Restatement (Second) of Torts § 652 (Am. L. Inst. 1977)	15, 17
---	--------

CONSTITUTIONAL PROVISIONS

Ill. Const. 1970, Art. I, § 6	5
-------------------------------------	---

INTRODUCTION

This lawsuit challenges a company's dragnet data-collection business, which thwarts Illinois' laws and public policies protecting the privacy of its immigrant residents. LexisNexis Risk Solutions ("LexisNexis")¹ seeks to avoid accountability. But complain as it might, this company violates Plaintiffs' privacy rights by creeping along their digital paths, collecting their personal information, aggregating it, selling it to federal immigration authorities and profiting—all while refusing to allow consumers to opt out.

The state of Illinois, Cook County, and the City of Chicago have all acknowledged that exposing their immigrant residents' sensitive information to Immigration and Customs Enforcement (ICE) will put them at risk. Thus, all have taken steps to ensure that this data is protected, and that ICE does not have unfettered access to it. Despite this, LexisNexis invades Plaintiffs' privacy rights in violation of Illinois statutory and common law, and now falsely claims no such rights exist in an attempt to protect its lucrative business model.

LexisNexis' arguments for dismissing the Complaint lack merit. As the Supreme Court has unequivocally stated, "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *Brooks v. Thomson Reuters Corp.*, No. 21-cv-01418-EMC, 2021 WL 3621837, at *8 (N.D. Cal. Aug. 16, 2021) (quoting *U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989) (denying motion to dismiss unfair business practice claim against data broker Thomson Reuter for conduct indistinguishable from that of LexisNexis). This Court should deny LexisNexis' motion to dismiss.

¹ LexisNexis notes that its full and complete name is "LexisNexis Risk Solutions, Inc." Plaintiffs request leave to amend their complaint to reflect this should the Court determine it is necessary.

FACTUAL BACKGROUND

LexisNexis amasses vast amounts of sensitive personal data on U.S. consumers, including Illinoisans. Compl. ¶ 17. In fact, it claims to have constructed 276 million profiles on U.S. adults. *Id.* ¶ 3. It packages this data in dossiers offering an encyclopedic summary of a person's identity and sells them to private and public entities. *Id.* ¶¶ 2, 20-23, 66. LexisNexis does not seek consent from—or even inform—affected consumers, and flatly refuses to allow them to opt out when their data is compiled on behalf of law enforcement customers like ICE. *Id.* ¶¶ 18, 77.

LexisNexis pulls from both public and non-public sources of information to create its dossiers. *Id.* ¶¶ 20-23. Non-public information includes unredacted Social Security numbers, immigration status set out in driver records, as well as license plate reader data and incarceration data that can be used to track a person's movements and location, both historically and in real-time. *Id.* ¶¶ 4, 21, 48. It also includes non-public information derived from purchases of essential utilities and telecom services, including up-to-date addresses, which can be used to locate and deport noncitizen residents. *Id.* ¶¶ 21, 23.² The dossiers also contain embarrassing and disparaging information, such as derogatory photos and inaccurate information. *Id.* ¶¶ 26, 32, 106. For example, Plaintiff Castellanos' profile lists a wrong Social Security number, causing her to fear allegations that she fraudulently used another's Social Security number. *Id.* ¶ 67. Such inaccuracies also increase the risk of misidentification. *Id.* ¶ 61. LexisNexis even publishes speculative associations based on perceived, and sometimes inaccurate, romantic, family, or other relationships (including ones that people may not want publicized). *Id.* ¶¶ 67, 73. The

² This information and more may come from proprietary sources, including but not limited to insurance, phone, employment, utilities, renter information, licenses, and credit checks. *Id.* ¶ 50.

company updates its information in real time. *Id.* ¶ 22. In other words, LexisNexis tracks us from the cradle to the grave and contains information revealing virtually everything about our lives.

LexisNexis sells its invasive dossiers to law enforcement agencies, including ICE. *Id.* ¶¶ 5, 17, 35. Using these, ICE can target individuals for immigration enforcement based on information it would not, in many cases, otherwise be able to obtain without a subpoena, court order, or other legal process. *Id.* ¶¶ 5, 53. Indeed, in ICE’s contracting documents with LexisNexis, the agency explicitly stated that it needs real-time incarceration data that state and local governments no longer share under their “sanctuary” laws. *Id.* ¶ 51. In other words, LexisNexis allows law enforcement to circumvent the laws places like Illinois have enacted to protect Plaintiffs and others like them.³

LexisNexis deprives Plaintiffs of the economic value of their data and privacy. *Id.* ¶ 93. LexisNexis’ business model demonstrates that this information has concrete value. Specifically, LexisNexis charges for individual reports compiling this private information, and leverages access to the data to charge subscription fees. *Id.* ¶ 36. It thus earns money by creeping behind us online, collecting and aggregating our private information, and then selling it without consent or compensation. *Id.* ¶ 97. And of course, LexisNexis does all of this to Plaintiffs in particular. *Id.*

Individual and Organizational Plaintiffs brought this action to stop LexisNexis from invading their privacy and exploiting their sensitive information, thus depriving them of the economic value of their data and the ability to control that data (and often mischaracterizing that data, causing other harms), chilling their core constitutional rights of freedom of association and

³ LexisNexis does not dispute that Plaintiffs never consented to its use of their personal data. Rather, it touts the utility of its products as effective law enforcement tools. Mot. 3. Whether or not this conclusory assertion is true (and it is not clear that it is) matters not. Selling products (even to law enforcement) that are tortious at their inception is unlawful. Further, given the lack of judicial oversight, LexisNexis’ sale of this data to law enforcement constitutes a grave threat to civil liberties.

speech, and causing injury to their peace of mind and well-being. Individual Plaintiffs also seek damages and disgorgement of profits resulting from the sale of this information.

I. ARGUMENT

LexisNexis asserts that Plaintiffs have no right to privacy with respect to their personal information. Mot. 4. Nothing could be further from the truth. Indeed, the Supreme Court has recognized that the dissemination of personal information constitutes a profound privacy violation. *See, e.g., U.S. Dep't of Def. v. Fed. Lab. Rels. Auth.*, 510 U.S. 487, 501 (1994) (finding that employees “have *some* nontrivial privacy interest in nondisclosure [of addresses]”); *Reps. Comm. For Freedom of Press*, 489 U.S. at 749–50, 764 (nonconsensual dissemination of “rap sheets” constituted “an unwarranted invasion of privacy”); *U.S. Dep't of State v. Ray*, 502 U.S. 164, 175–76 (1991) (same with respect to unauthorized dissemination of “highly personal information regarding marital and employment status, children, living conditions and attempts to enter the United States”). Crucially, even the dissemination of purely public information can constitute a significant invasion of privacy, particularly when the information is aggregated, heightening privacy concerns. *Reps. Comm. For Freedom of Press*, 489 U.S. at 764 (finding a “distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole”). The Supreme Court has also identified heightened privacy interests in data aggregated over significant periods of time that reveals one’s historical movements and location. *See, e.g., Carpenter v. United States*, 138 S. Ct. 2206, 2217–20 (2018).

Illinois specifically recognizes and safeguards the right to privacy. *See* Ill. Const. art. I, § 6 (providing state residents with protection from “invasions of privacy”); *Hope Clinic for Women, Ltd. v. Flores*, 991 N.E.2d 745, 761 (Ill. 2013) (noting that “the Illinois Constitution

goes beyond Federal constitutional guarantees by expressly recognizing a zone of personal privacy”) (citation omitted); *Leopold v. Levin*, 259 N.E.2d 250, 254 (Ill. 1970) (recognizing rights to privacy as “sensitive and necessary human values”).

Illinois and local governments within the state also rigorously protect this right for their vulnerable immigrant residents. For example, the Illinois TRUST Act, Cook County’s Detainer Ordinance, and Chicago’s Welcoming City Ordinance each restrict ICE’s access to information about immigrants and specifically protect incarceration data, including information pertaining to the timing of a person’s release. *See, e.g.*, Illinois TRUST Act, 5 Ill. Comp. Stat. § 805/15(e), (h)(6)-(7) (providing, inter alia, that law enforcement officers generally should not inquire about immigration status or provide information about people in custody to ICE, including release dates); Cook County’s Detainer Ordinance, Cook County, Ill., Code of Ordinances ch. 46, art. II, div. 1, subdiv. I, § 46-37(b) (generally preventing Sheriff from communicating information, such as incarceration status or release date, to ICE); Chicago’s Welcoming City Ordinance, Chi., Ill., Municipal Code of Chicago §§ 2-173-020, 2-173-030, 2-173-042(b)(1)(C) (generally limiting information gathering and dissemination relating to immigration status and preventing law enforcement communication with ICE regarding custody status or release dates).

Plaintiffs’ detailed complaint plainly specifies facts sufficient to allege violations of the Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA), as well as the common law protections against intrusion upon seclusion and unjust enrichment. LexisNexis conveniently ignores parts of Plaintiffs’ complaint and mischaracterizes others. It does so in the face of a complaint that plainly states these claims.

A. The complaint sufficiently alleges LexisNexis’ conduct violates the ICFA.

- 1. Plaintiffs have an obvious “consumer nexus” to LexisNexis’ unfair business practice of gathering, aggregating, and selling their private data to third parties.**

Contrary to LexisNexis' contentions, Plaintiffs have alleged facts sufficient to satisfy the "consumer nexus test." The ICFA provides a cause of action to "[a]ny person who suffers actual damage as a result of a violation of th[e] Act committed by any other person[.]" 815 Ill. Comp. Stat. § 505/10a(a). "[T]he legislature has mandated that [ICFA] is to be liberally construed to effectuate its purposes." *Bank One Milwaukee v. Sanchez*, 783 N.E.2d 217, 220 (Ill. App. Ct. 2003) (citing 815 Ill. Comp. Stat. § 505/11a).

Courts in this district have held that a consumer nexus can be established through "a showing of 'trade practices directed to the market generally' or that the conduct [at issue] 'otherwise implicates consumer protection concerns.'" *Frazier v. U.S. Bank Nat'l Ass'n*, No. 11 C 8775, 2013 WL 1385612, at *4 (N.D. Ill. Apr. 4, 2013) (quoting *Athey Prods. Corp. v. Harris Bank Roselle*, 89 F.3d 430, 437 (7th Cir. 1996)). It is "a near certainty that" LexisNexis has a dossier on "anyone who has a consumer footprint in the United States". Compl. ¶ 72. LexisNexis' massive and systematic exploitation of consumers' personal information without consent and compensation is "directed to the market generally."

Furthermore, LexisNexis' use and misuse of individuals' personal data and invasions of privacy certainly concern consumer protection laws because they harm consumers. *See infra* Section I(A)(2); *see also In re Michaels Store Pin Pad Litig.*, 830 F.Supp.2d 518, 525-26 (N.D. Ill. 2011) (finding sufficient allegation of ICFA violation based on company's failure to safeguard plaintiff's private information). LexisNexis claims effective ICFA immunity because its sales of Accurint are primarily to government entities and businesses, not to individuals. But adoption of that reasoning would gut consumer protections in many contexts, including the data privacy context, where business-to-business transactions harm ordinary consumers and private individuals, and enrich the businesses. *Id.* To shield businesses from liability for their harms to

individuals because of contracts that public entities enter into would render ICFA a dead letter in all such transactions. This conflicts with Illinois law that a consumer nexus exists where business practices “implicate[] consumer protection.” *Frazier*, 2013 WL 1385612, at *4. Finally, LexisNexis’ practices also implicate consumer protection because much of the information in its dossiers directly derives from consumer activities—including records from credit agencies, DMV records, cellphone registries, property records, and utility accounts. *Id.* ¶¶ 64-69, 72, 91.

LexisNexis attempts to argue that *purchasers* of Accurint suffer no harm and therefore Plaintiffs’ ICFA claim should fail. Mot. 5. This is incorrect, but also does not matter. As shown above, the key to the consumer nexus test is the damage to all Illinoisans, including Plaintiffs. Moreover, LexisNexis fails to acknowledge that Accurint *customers*, including Cook County officials and ICE agents employed by the Chicago ICE field office, inevitably are among those subjected to LexisNexis’ nonconsensual practices: this company compiles profiles on “anyone who has a consumer footprint in the United States[.]” Compl. ¶¶ 40, 47, 72. Those Illinoisans’ rights are violated too.

While most federal courts apply the consumer nexus test as stated in *Frazier* and *Athey Prods. Corp.*, some courts apply a test with different criteria. *See, e.g., Glob. Total Off. Ltd. P’ship v. Glob. Allies, LLC*, No. 10 C 1896, 2011 WL 3205487, at *2 (N.D. Ill. July 28, 2011). This test states that a consumer nexus is established when a plaintiff demonstrates “(1) that [its] actions were akin to a consumer’s actions to establish a link between [it] and consumers; (2) how defendant’s representations ... concerned consumers other than [plaintiff]; (3) how defendant’s particular [action] involved consumer protection concerns; and (4) how the requested relief would serve the interests of consumers.” *Id.*

Plaintiffs also easily meet this test. *First*, Plaintiffs engaged in consumer activities, such as purchasing utilities, renting or purchasing their residences, or obtaining documents from the Illinois' Driver Services Department that link them to consumers of LexisNexis' products whose consumer information is also collected, aggregated and sold by the company without their consent. Compl. ¶¶ 8-12. *Second*, LexisNexis' conduct affects nearly every adult in the U.S., not only Plaintiffs. *Third*, LexisNexis' practices result in a non-consensual, all-encompassing invasion of privacy of nearly all U.S. consumers, including purchasers of LexisNexis' products, with no opt-out opportunity. This implicates consumer protection as explained above. *Fourth*, by enjoining LexisNexis' practices, nearly all adult consumers in the U.S., including purchasers of the company's products, will be protected against an all-encompassing invasion of their privacy.⁴

2. Plaintiffs have adequately alleged LexisNexis' conduct qualifies as an unfair business practice under the ICFA.

LexisNexis' conduct is unfair because (1) it offends public policy; (2) it rises to the level of oppressive or immoral conduct; and (3) it causes substantial injury to consumers. *See Robinson v. Toyota Motor Credit Corp.*, 775 N.E.2d 951, 961 (Ill. 2002). While courts review each of the above factors, "[a]ll three criteria do not need to be satisfied to support a finding of unfairness. [Rather a] practice may be unfair because of the degree to which it meets one of the criteria or because to a lesser extent it meets all three." *Id.* (internal citations omitted). The test measures the totality of LexisNexis' conduct.

⁴ To argue that Plaintiffs have not alleged a nexus, LexisNexis makes several inaccurate assertions. For example, it claims that "ICFA only covers claims of consumer fraud." Mot. 5. Not so. The statute protects against unfair practices, in addition to fraudulent or deceptive ones. Relatedly, LexisNexis also misstates the pleading standard for an ICFA claim that *does not* lie in fraud, as here. *Id.* at 6. This Court has consistently held that Rule 9(b) dismissal is only available for an ICFA claim "[i]f the claim rests on allegations of deceptive conduct[.]" *Totty v. Anderson Funeral Home, Ltd.*, 448 F. Supp. 3d 928, 936 (N.D. Ill. 2020) (Rowland, J.). Plaintiffs here are not alleging deceptive conduct or fraud and easily satisfy the applicable standard.

In terms of harm to consumers, LexisNexis’ creeping, collecting, aggregating and selling U.S. consumers’ sensitive personal and often non-public data causes substantial injury. Indeed, the harm here violates quintessential privacy rights safeguarded by consumer protection laws. *See Brooks*, 2021 WL 3621837. In *Brooks*, the Court evaluated conduct indistinguishable from LexisNexis’ under California’s Unfair Competition Law (UCL).⁵ There, the Court observed:

[T]he harm to Plaintiffs is tremendous: an all-encompassing invasion of Plaintiffs’ privacy, whereby virtually everything about them—including their contact information, partially redacted social security number, criminal history, family history, and even whether they got an abortion, to name just a few—is transmitted to strangers without their knowledge, let alone their consent[.]

Brooks, 2021 WL 3621837 at *8.

The *Brooks* court went on to explain that the dissemination of personal data and, in particular, “[the compilation of] disparate pieces of information . . . into a single dossier” conducted by Thomson Reuter constituted “a significant invasion of privacy” under various Supreme Court precedents. *Id.* at *9.

Plaintiffs’ economic injury alone, resulting from LexisNexis exploiting their data without compensation, is also significant. While the economic injury to each Plaintiff may be small, LexisNexis invades the lives of nearly all adults in the United States and in the process assembles a massive economic benefit. *Centerline Equip. Corp. v. Banner Pers. Serv., Inc.*, 545 F. Supp. 2d 768, 780 (N.D. Ill. 2008) (very small individual harms were substantial because they

⁵ While *Brooks* analyzed the California UCL, rather than the ICFA, the *Brooks* Court’s analysis is relevant here because the concept of unfairness in both statutes parallels section 5 of the Federal Trade Commission (FTC) Act (15. U.S.C. § 45). *Compare People v. Nat’l Ass’n of Realtors*, 174 Cal. Rptr. 728, 737 (Cal. Ct. App. 1981) (section 5 of the FTC Act is the “federal equivalent of [California’s] unfair competition statutes”) and *People ex rel. Mosk v. Nat’l Rsch. Co. of Cal.*, 20 Cal. Rptr. 516, 522 (Cal. Dist. Ct. App. 1962) (federal court decisions interpreting section 5 are “more than ordinarily persuasive” in construing the UCL) with, e.g., 815 Ill. Comp. Stat. § 505/2 (courts construing the ICFA shall give “consideration . . . to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act.”); *Robinson*, 775 N.E.2d at 960-61 (relying on factors for determining unfairness promulgated under section 5 of the FTC Act to determine whether an ICFA violation had occurred).

are “part of a practice that, in the aggregate, causes substantial losses to the public as a whole”) (internal citation omitted).

In addition to the harm caused by this “all-encompassing” invasion of privacy, LexisNexis’ conduct offends Illinois public policy at the state and local levels. A business practice offends public policy when it falls “within at least the penumbra of some common-law, statutory, or other established concept of unfairness.” *People ex rel. Fahner v. Hedrich*, 438 N.E.2d 924, 929 (Ill. App. Ct. 1982) (quoting *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 n.5 (1972)) (finding practice to offend public policy even where no cited law barred the practice); *see also Sperry & Hutchinson Co.*, 405 U.S. at 244, 244 n.5 (determining whether a practice is unfair may involve “consider[ing] public values beyond simply those enshrined in the letter or encompassed in the spirit of . . . laws”); *Spiegel, Inc. v. FTC*, 540 F.2d 287, 291-94 (7th Cir. 1976) (determining that a business practice could be deemed unfair despite assuming *arguendo* that the practice was legal).

Here, as detailed below, LexisNexis’ practices constitute intrusion upon seclusion and unjust enrichment, thus violating Illinois law. But even if that were not so, LexisNexis’ practices are unfair because they thwart “the public values” in Illinois, established by ample evidence of policies to protect against egregious violations of privacy. Illinois enshrines its protection against privacy violations in its legislation, its Constitution, and its common law. *See supra* Part I.

Importantly, LexisNexis’ data sharing with ICE and law enforcement also upends state and local policies intended to protect the privacy and civil rights of immigrant communities, including the Illinois TRUST Act, Cook County’s Detainer Ordinance, and Chicago’s Welcoming City Ordinance. Compl. ¶ 53. Under these laws, law enforcement agencies and other agencies must deny ICE’s requests to provide information on or detain immigrants, but

LexisNexis' practices serve as a backdoor, allowing ICE to determine a person's immigration status from their driver records or use real-time jail data to arrest immigrants as they are being released. LexisNexis is, therefore, facilitating ICE's circumvention of these laws and ordinances. The whole point of these laws is to constrain law enforcement and other government data sharing in various ways to protect the rights and interests of Illinois residents. LexisNexis thwarts those policies by selling a means for law enforcement to evade state limits, directly threatening the precise interests that Illinois and its local municipalities meant instead to protect. That these laws and ordinances do not explicitly apply to private companies is irrelevant. Illinois' public policy favors protecting residents' privacy against ICE. A company violates ICFA when it sells a product that directly harms Illinois' policy interests.

LexisNexis' conduct also undermines the public policy goals of the Illinois Personal Information Protection Act (PIPA). The PIPA sets forth detailed steps data collectors must take when "personal information" is breached, including notifying affected individuals and taking appropriate data security measures. 815 Ill. Comp. Stat. § 530/5. The PIPA defines personal information to include a person's name in combination with an identification number, including a Social Security or driver's license number, the exact type of information at issue here. *Id.*⁶ The PIPA thus reflects a strong public policy against unauthorized dissemination of Social Security numbers and other identifying data. That LexisNexis sells that same data without consent or knowledge of the people affected defeats PIPA and its purposes.

LexisNexis argues that it complies with state and federal laws, Mot. 7, but this is highly questionable.⁷ First, LexisNexis' conduct violates the ICFA and constitutes a tort under Illinois

⁶ Certain tailored Accurint products including for insurers and healthcare organizations may provide access to medical records, which are also protected under PIPA. Compl. ¶ 35.

⁷ Contrary to LexisNexis' assertions, its practices are contrary to federal laws that were enacted to protect consumers' data—laws that specifically create safeguards so that law enforcement is unable to misuse or access

common law. *See infra* Sections I(B-C). Additionally, LexisNexis has settled multiple lawsuits for violations of federal laws, such as the Driver's Privacy Protection Act (DPPA) (18 U.S.C. § 2721) (2000) and the Fair Credit Reporting Act (FCRA) (15 U.S.C. §§ 1681 et seq.), including at least one case in which a court found the company violated DPPA as a matter of the law.⁸ But even LexisNexis' technical compliance with some federal and state laws would not absolve it of its clear offenses against public policy discussed herein.

LexisNexis also engages in oppressive or immoral conduct. Business practices may be oppressive under the ICFA where they "impose[] a lack of meaningful choice or an unreasonable burden on its target." *Centerline*, 545 F. Supp. 2d at 780. Here, consumers have no meaningful opportunity to escape LexisNexis' data creeping, collecting, and selling. They are unduly burdened by it, as most people are unaware it is happening and cannot protect themselves. Further, LexisNexis' opt-out measures are limited and riddled with exemptions, particularly with respect to law enforcement tools, where there is no opt out at all. Compl. ¶ 77. This conduct is immoral too given the associated harms, its upending of public policy, and its oppressive nature.⁹

3. Plaintiffs adequately pled actual damages.

LexisNexis finally argues that Plaintiffs' ICFA claim fails due to the requirement to plead actual damages. Mot. 8. LexisNexis wholly ignores Plaintiffs' allegation that "LexisNexis has

sensitive data without making the requisite showing of reasonableness. *See, e.g.*, 18 U.S.C. §§ 2702-2703 (limiting ability of government actors to access subscriber information from covered internet and email service providers without a subpoena); 47 U.S.C. § 551 (barring a cable service provider from releasing the personally identifiable information of a cable subscriber to a government entity without a court order).

⁸ *Gaston v. LexisNexis Risk Sols., Inc.*, 483 F. Supp. 3d 318, 346 (W.D.N.C. 2020) (granting summary judgment for plaintiffs for DPPA violations). Cases LexisNexis has settled include *Gaston v. LexisNexis Risk Sols., Inc.*, No. 5:16-cv-00009-KBD-DCK, 2021 WL 2077812 (W.D.N.C. May 24, 2021) (approving over \$5 million settlement agreement) and *Berry v. LexisNexis Risk & Info. Analytics Grp., Inc.*, No. 3:11-CV-754, 2014 WL 4403524 (E.D. Va. Sept. 5, 2014) (approving over \$13.5 million settlement agreement over alleged FCRA violations).

⁹ LexisNexis takes issue with Plaintiffs' reliance on *Newman v. Metro. Life Ins. Co.*, 885 F.3d 992, 1002–03 (7th Cir. 2018) in the Complaint because *Newman* is factually distinct from Plaintiffs' case in terms of the method used to achieve oppressive circumstances. This is a distinction without a difference, because in both cases, the end result is a situation where the plaintiffs lack any meaningful choice.

deprived them of the economic value of their sensitive information.” Compl. ¶ 93. LexisNexis also fails to cite any authority that undermines Plaintiffs’ argument.¹⁰

In this new era of virtual data collection, courts have increasingly recognized the loss of the opportunity to profit from one’s private data as a cognizable economic injury. *See, e.g., Kellman v. Spokeo, Inc.*, No. 3:21-cv-08976-WHO, 2022 WL 1157500, at *10 (N.D. Cal. Apr. 19, 2022) (plaintiffs’ allegations that they were not compensated for their data qualified as economic injury under the UCL); *Callahan v. PeopleConnect, Inc.*, No. 20-cv-09203-EMC, 2021 WL 5050079, at *19 (N.D. Cal. Nov. 1, 2021) (same); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) (collecting cases); *see also Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1247 (7th Cir. 2021) (a plaintiff could establish injury required for standing where she “assert[s] . . . that by selling her data, the collector has deprived her of the opportunity to profit from her . . . information.”). Recognizing this economic injury allows courts to redress harm caused by the new and novel ways companies are monetizing consumers’ personal data.¹¹

LexisNexis makes significant profits through its charges for individual reports, placing a concrete value on the information included in a particular dossier. The fact that LexisNexis profits from Plaintiffs’ data distinguishes this case from those involving a data breach where there is nothing more than a hypothetical diminution in the value of data resulting from a disclosure to unknown persons or entities. Instead, this case is akin to others where, as here, a company is monetizing its own collection of individuals’ personal data without consent or

¹⁰ In addition to suffering economic injury, Plaintiffs also allege that they suffer other “immediate and irreparable injuries, including the chilling of their core constitutional rights of freedom of association and freedom of speech, violations of their rights to privacy, . . . and injuries to their peace of mind and well-being.” *Id.* ¶ 79.

¹¹ That the injury suffered by a consumer in such cases may be small is of no significance. *Centerline*, 545 F. Supp. 2d at 779 (“This may be a minute injury, but it is an injury nonetheless.”).

compensation to the people affected. *See, e.g., Kellman*, 2022 WL 1157500, at *1-2; *Callahan*, 2021 WL 5050079, at *1. Plaintiffs have sufficiently alleged their ICFA claim.

B. Plaintiffs Sufficiently Plead Their Claim for Unjust Enrichment.

Plaintiffs satisfy the test for unjust enrichment based on third party behavior. Factors giving rise to unjust enrichment under these circumstances include the following:

(1) the benefit should have been given to the plaintiff, but the third party mistakenly gave it to the LexisNexis instead, (2) the LexisNexis procured the benefit from the third party through some type of wrongful conduct, or (3) the plaintiff for some other reason had a better claim to the benefit than the LexisNexis.

HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc., 545 N.E.2d 672, 679 (Ill. 1989) (internal citations omitted).¹²

Plaintiffs have adequately pled facts demonstrating LexisNexis' conduct is both wrongful and that they have a better claim to the value of their data than LexisNexis.

LexisNexis argues that its conduct does not "violate any laws" and therefore cannot be wrongful. Plaintiffs, however, have established that LexisNexis' conduct is tortious and violates the ICFA. Moreover, contrary to LexisNexis' assertion, conduct need not violate the law to be considered wrongful. *Midcoast Aviation*, 907 F.2d at 738 n.3 ("Wrongfulness' does not mean that a defendant must perform illegal acts or manifest signs of moral depravity. It means merely that a defendant does something unjust, thus making its enrichment unjust."). LexisNexis' practice of collecting, aggregating, and selling consumers' personal information without consent and compensation deeply violates privacy and is therefore wrong and unjust.

Also, LexisNexis incorrectly claims that Plaintiffs have no plausible claim that they are entitled to profits LexisNexis generates by selling their data. Plaintiffs' personal data clearly has

¹² However, conditions of unjust enrichment based on third party conduct are not limited to those discussed in *HPI*. *See Midcoast Aviation, Inc. v. Gen. Elec. Credit Corp.*, 907 F.2d 732, 738 n.3 (7th Cir. 1990).

economic value. Otherwise, LexisNexis would not be selling it. *See supra* Section I(A)(3). Indeed, Accurant would be worthless without the vast amounts of underlying data it contains. LexisNexis is creeping, collecting, aggregating, and selling this data without consent or compensation in violation of the law. Thus, Plaintiffs have a greater claim to the profits than LexisNexis, who obtained these profits through acts constituting intrusion upon seclusion and unfair business practices.¹³ For the above reasons, Plaintiffs state a claim for unjust enrichment.

C. Plaintiffs Sufficiently Plead Their Claim for Intrusion Upon Seclusion.

LexisNexis' conduct in collecting, aggregating, and selling Plaintiffs' personal information without consent and compensation meets the elements of intrusion upon seclusion.

Intrusion upon seclusion occurs where, as here: (1) a defendant commits an unauthorized intrusion or prying into the plaintiff's seclusion; (2) the intrusion would be highly offensive or objectionable to a reasonable person; (3) the matter intruded on was private; and (4) the intrusion caused the plaintiff anguish and suffering. *See Johnson v. K mart Corp.*, 723 N.E.2d 1192, 1196 (Ill. App. 2000). Contrary to LexisNexis' assertion that the "tort requires the physical intrusion upon a plaintiff's property[.]" Mot. 10, a defendant might invade privacy through surveillance or "by some other form of investigation or examination" into private matters. *Lawlor v. N. Am. Corp. of Ill.*, 983 N.E.2d 414, 424 (Ill. 2012) (quoting and following Restatement (Second) of Torts § 652B cmt. b (Am. L. Inst. 1977)). Indeed, non-physical intrusions of a similar nature to the collection and aggregation of data here, such as eavesdropping, may be far more intrusive than physical ones, such as "searching someone's shopping bag[.]" Mot. 11.

¹³ Additionally, LexisNexis argues that Plaintiffs' unjust enrichment claim is premised on the same conduct as its ICFA and intrusion upon seclusion claims and therefore unjust enrichment is not a standalone cause of action. Mot. 8. However, this Court need not determine whether unjust enrichment constitutes a standalone cause of action at this stage because Plaintiffs have alleged facts that demonstrate a violation of the ICFA and meet the elements of common law intrusion upon seclusion.

LexisNexis first argues that Plaintiffs have not demonstrated an unauthorized intrusion. Not so. By pleading that each Individual Plaintiff has taken steps to protect their sensitive private information and that LexisNexis nevertheless collected, aggregated and used their personal data without consent and compensation, Plaintiffs established an unauthorized intrusion. By engaging in these surreptitious profit-making activities, LexisNexis intruded on Plaintiffs by “investigation or examination” into their private affairs.

LexisNexis’ argument that its activities do not constitute an unauthorized intrusion relies heavily on *In re Trans Union Corp. Priv. Litig.*, 326 F. Supp. 2d 893 (N.D. Ill. 2004). But while the Court in *Trans Union* found that the credit reporting agency at issue had not committed an unauthorized intrusion, the facts in that case are distinguishable. Crucial to *Trans Union*’s analysis was the fact that the “Plaintiffs do not and cannot allege that they were unaware that their creditors would pass th[eir] information on to Trans Union in the normal course of business.” *Id.* at 902. In stark contrast, here, as in “the vast majority of cases, consumers do not know that LexisNexis has collected their personal information and data, let alone that it is selling this information for profit.” Compl. ¶ 18. Whereas the plaintiffs in *Trans Union* would logically assume that their creditors would be providing their credit information to a credit reporting agency, Plaintiffs here would have no reason to suspect that LexisNexis is creeping after their everyday digital trails, collecting and buying up vast amounts of data about them, using that to create its own identification system of virtually every adult in the United States, and then selling that information for profit to private and public entities, including ICE. *Trans Union* could not be more different. It involved the compilation of some consumer information sold to marketers, rather than the compilation of encyclopedic dossiers sold to law enforcement agencies.

LexisNexis creates cradle-to-grave dossiers that track consumers' activities throughout their entire lives. LexisNexis' troubling data collection dwarfs the concerns raised by the discrete data collected and shared in *Trans Union*. Cf. *Carpenter*, 138 S. Ct. at 2217-20 (finding privacy intruded on where “sophisticated” technology “exhaustive[ly] chronicle[d]” data from services “indispensable to participation in modern society”) (citation omitted).

Following the Restatement (Second) of Torts, courts have increasingly recognized that collecting individuals' information without their consent may constitute an unauthorized intrusion. See, e.g., *McDonald v. Kiloo ApS*, 385 F.Supp.3d 1022, 1034-36 (N.D. Cal. 2019) (plaintiffs asserting an intrusion involving a “commercial entity that secretly harvests” personal data stated cognizable claim); *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 293-94 (3d Cir. 2016) (same where “defendants tracked their online behavior without their permission to do so”); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072-77 (N.D. Cal. 2016); *Calhoun*, 526 F. Supp. 3d at 629-31. This court should follow this trend and recognize that LexisNexis' aggregation and collection of Plaintiffs' data constitutes an unauthorized intrusion.

LexisNexis next argues that Plaintiffs have not established that LexisNexis' creeping, collecting, and prying into their affairs is “highly offensive or objectionable to a reasonable person.” LexisNexis does so by cherry-picking allegations from the complaint in an attempt to characterize Plaintiffs as taking issue solely with the *publication* or *dissemination* of their personal information, rather than LexisNexis' *collection* and *aggregation* of that data. In fact, Plaintiffs allege that the *collection* of their information is highly offensive and objectionable. As the complaint explains with respect to the extensive dossiers LexisNexis compiled on Individual Plaintiffs, LexisNexis' “*collection* of this personal data is cause for grave concern and highly offensive.” Compl. ¶ 70; see also *id.* ¶ 17 (records “amasse[d] . . . from the most intimate corners

of our lives”); *id.* ¶ 18 (collection is done surreptitiously and non-consensually); *id.* ¶¶ 21-25, 50 (describing public and private records searched). Moreover, the Complaint further states that “[t]he *collection and aggregation* of this information that Plaintiffs are trying to protect and keep private is highly offensive . . . because it is an all-encompassing invasion of their privacy” and includes . . . “erroneous information that is misleading and/or embarrassing,” such as former romantic partners, and inaccurate Social Security numbers. *Id.* ¶ 106 (emphasis added); *see also id.* ¶ 67.

LexisNexis make no attempt to show why the egregious invasion of privacy caused by the *collection and aggregation* of Plaintiffs’ data would not be highly offensive or objectionable to a reasonable person. Nor do they cite any relevant authorities on this point.

Lastly, LexisNexis argues that the information that it intruded upon is not private. Mot. 13. But much of the data LexisNexis collects and aggregates comes from non-public sources. Compl. ¶¶ 4, 20-23, 45. Also, the data LexisNexis collects and aggregates includes inaccurate information that may be misleading and information that may be embarrassing, such as bad credit, lien, and bankruptcy information, derogatory photos, information about one’s romantic relationships, incarceration status, name changes (particularly for transgender people), as well as sensitive information revealing a person’s immigration status from driver records, information about family relationships and healthcare, and location data from license plate readers or jails. Courts have determined that these types of sensitive private information should be protected by tort law. *See, e.g., In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019) (“detailed dossiers” including “photos . . . [information on] relationships, and information that could reveal location” deemed private facts in motion to dismiss context); *Gross v. Chapman*, 475 F. Supp. 858, 862-63 (N.D. Ill. 2020) (discussing Illinois federal and

state decisions where, inter alia, information on topics such as “healthcare, finances, and family” and “romantic relationships” was deemed private).

LexisNexis cites cases that purport to define what constitutes private versus non-private information. But those cases did not deal with several of the types of information at issue here, such as derogatory photos, information about an individual’s romantic relationships, and family history, misleading information, and information revealing a person’s location.

Moreover, none of those cases dealt with the aggregation of data into encyclopedic dossiers. As the Supreme Court has recognized, privacy interests in one’s data are heightened where disparate pieces of information are compiled, even when the underlying information is publicly available. *Reps. Comm. For Freedom of Press*, 489 U.S. at 763-64. Thus, even if the individual pieces of information that LexisNexis collects might not be considered private in isolation, LexisNexis’ aggregation of information containing “virtually everything about” Plaintiffs renders the information private. *Brooks*, 2021 WL 3621837, at *8. Plaintiffs have sufficiently alleged their intrusion upon seclusion claim.

D. Plaintiffs Sufficiently Alleged Facts Establishing Associational Standing.

LexisNexis’ argument that the Organizational Plaintiffs do not meet the requirements of associational standing rests on an apparent confusion regarding the relief these Plaintiffs seek. LexisNexis incorrectly asserts that the Organizational Plaintiffs are seeking damages on behalf of their members. Mot. 14.¹⁴ The Complaint clearly states that the Organizational Plaintiffs “participate[] as [] plaintiff[s] only for purposes of securing declaratory and injunctive relief.”

¹⁴ LexisNexis also challenges Plaintiffs declaratory relief cause of action as duplicative of relief sought in other claims. Mot. 13-14. Should this Court agree that the cause of action is duplicative, Plaintiffs request leave to amend that cause of action to address this issue.

Compl. ¶¶ 11-12. Thus, *Duncan Place Owners Ass’n v. Danze, Inc.*, 927 F.3d 970, 978 (7th Cir. 2019), cited by LexisNexis, is inapposite, as the Associational Plaintiff there sought damages.

“[S]o long as the nature of the claim and of the relief sought does not make the individual participation of each injured party *indispensable* to proper resolution of the cause, [an] association may be an appropriate representative of its members, entitled to invoke [a] court’s jurisdiction.” *Warth v. Seldin*, 422 U.S. 490, 511 (1975) (emphasis added). Organizational Plaintiffs have identified members in the complaint who have individual standing to sue. Compl. ¶¶ 73-74.¹⁵ Here, Organizational Plaintiffs claim that LexisNexis’ practices cause widespread harms affecting nearly every adult in the United States based on their consumer transactions by, at a minimum, depriving them all of the economic value of their private information, and they only seek declaratory and injunctive relief. There is thus no need here for the Court to engage in an individualized assessment of Plaintiffs’ members. *See McConchie v. Scholz*, 567 F. Supp. 3d 861, 880 (N.D. Ill. 2021) (quoting *Retired Chi. Police Ass’n v. City of Chicago*, 7 F.3d 584, 603 (7th Cir. 1993)) (“Declaratory, injunctive, or other prospective relief will usually inure to the benefit of the members actually injured and thus individualized proof of damages is often unnecessary.”) (citation omitted). This is exactly the type of case where the nature of the claim and relief sought makes individual participation of members unnecessary.

CONCLUSION

For the reasons above, the Court should deny LexisNexis’ motions to dismiss. If, however, any claim is dismissed, Plaintiffs request leave to amend. *See* Fed. R. Civ. P. 15(a)(2).

¹⁵ Thus, *Prairie Rivers Network v. Dynegy Midwest Generation, LLC*, 2 F.4th 1002, 1009 (7th Cir. 2021), cited by LexisNexis, is inapposite. Moreover, even if this Court were to determine that some participation of Organizational Plaintiffs’ members was needed, that would not be fatal to associational standing. *Deerpath Consol. Neighborhood Ass’n v. Lake County Bd. of Review*, No. 2-19-0985, 2021 WL 5998539, at *4 (Ill. App. Ct. Dec. 20, 2021) (“Some member participation (such as providing evidence) is compatible with associational standing.”) (citing *Retired Chi. Police Ass’n*, 7 F.3d at 603).

Dated: November 14, 2022

Respectfully submitted,

/s/ Daniel Werner
One of the Plaintiffs' Attorneys

Sejal R. Zota*
sejal@justfutureslaw.org
Dinesh McCoy*
dinesh@justfutureslaw.org
Daniel Werner*
daniel@justfutureslaw.org
JUST FUTURES LAW
95 Washington Street, Suite 104-149
Canton, MA 02021
(617) 812-2822

Daniel Schneider
dschneider@legalactionchicago.org
LEGAL ACTION CHICAGO
Attorney No. 100037
120 S. LaSalle St., Suite 1000
Chicago, IL 60603
(312) 423-5941

**Admitted pro hac vice*

CERTIFICATE OF SERVICE

The undersigned, an attorney of record for the Plaintiffs, hereby certifies that on November 14, 2022 he served a copy of the foregoing Plaintiffs' Response in Opposition to Defendant's Motion to Dismiss on counsel of record for Defendant by electronic means pursuant to Electronic Case Filing (ECF).

/s/ Daniel Werner

Daniel Werner

JUST FUTURES LAW

95 Washington Street, Suite 104-149

Canton, MA 02021

(617) 812-2822